AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-24. (Canceled).

SUB C17

25. (Currently amended) A method for managing encryption within a database system, wherein encryption is performed automatically and transparently to a user of the database system, the method comprising:

receiving a request at the database system to store data in the database system;

wherein the request is directed to storing data in a portion of the database system that has been designated as encrypted;

in response to receiving the request:

~~,~~creating a digest of the data, and

automatically encrypting data within the database system using an encryption function to produce an encrypted data; and

B1

storing the encrypted data in the database system;

wherein the digest is used to detect tampering with the encrypted data.

26. (Previously presented) The method of claim 25,

wherein the portion of the database system that has been designated as encrypted includes a column of the database system;

wherein the encryption function uses a key stored in a keyfile managed by a security administrator; and wherein the encrypted data is stored using a storage function of the database system.

27. (Previously presented) The method of claim 26, further comprising:

receiving a request to retrieve data from the column of the database system;

if the request to retrieve data is received from a database administrator, preventing the database administrator from decrypting the encrypted data;

if the request to retrieve data is received from the security administrator, preventing the security administrator from decrypting the encrypted data; and

if the request to retrieve data is from an authorized user of the database system, allowing the authorized user to decrypt the encrypted data.

28. (Previously presented) The method of claim 26, wherein the security administrator selects one of, data encryption standard (DES) and triple DES as a mode of encryption for the column.

B1

29. (Previously presented) The method of claim 26, wherein the security administrator, a database administrator, and a user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles.

30. (Previously presented) The method of claim 26, wherein managing the keyfile includes, but is not limited to:

creating the keyfile;

establishing a plurality of keys to be stored in the keyfile;

establishing a relationship between a key identifier and the key stored in the keyfile;

storing the keyfile in one of,

an encrypted file in the database system, and

a location separate from the database system; and

moving an obfuscated copy of the keyfile to a volatile memory within a server associated with the database system.

31. (Previously presented) The method of claim 30, wherein the key identifier associated with the column is stored as metadata associated with a table containing the column within the database system.

32. (Previously presented) The method of claim 30, further comprising establishing encryption parameters for the column, wherein encryption parameters include encryption mode, key length, and integrity type by:

entering encryption parameters for the column manually; and

recovering encryption parameters for the column from a profile table in the database system.

31

33. (Previously presented) The method of claim 26, wherein upon receiving a request from the security administrator specifying the column to be encrypted, if the column currently contains data, the method further comprises:

decrypting the column using an old key if the column was previously encrypted; and

encrypting the column using a new key.

34. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer causes the computer to perform a method for managing encryption within a database system, wherein encryption is

performed automatically and transparently to a user of the database system, the method comprising:

receiving a request at the database system to store data in the database system;

wherein the request is directed to storing data in a portion of the database system that has been designated as encrypted;

in response to receiving the request:

~~,~~creating a digest of the data, and

automatically encrypting data within the database system using an encryption function to produce an encrypted data; and

storing the encrypted data in the database system~~;~~,

wherein the digest is used to detect tampering with the encrypted data.

35. (Previously presented) The computer-readable storage medium of claim 34,

31

wherein the portion of the database system that has been designated as encrypted includes a column of the database system;

wherein the encryption function uses a key stored in a keyfile managed by a security administrator; and

wherein the encrypted data is stored using a storage function of the database system.

36. (Previously presented) The computer-readable storage medium of claim 35, the method

further comprising:

receiving a request to retrieve data from the column of the database system;

if the request to retrieve data is received from a database administrator, preventing the database administrator from decrypting the encrypted data;

if the request to retrieve data is received from the security administrator, preventing the security administrator from decrypting the encrypted data; and

if the request to retrieve data is from an authorized user of the database system, allowing the authorized user to decrypt the encrypted data.

37. (Previously presented) The computer-readable storage medium of claim 35, wherein the security administrator selects one of, data encryption standard (DES) and triple DES as a mode of encryption for the column.

38. (Previously presented) The computer-readable storage medium of claim 35, wherein the security administrator, a database administrator, and a user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles.

B1

39. (Previously presented) The computer-readable storage medium of claim 35, wherein managing the keyfile includes, but is not limited to:

creating the keyfile;

establishing a plurality of keys to be stored in the keyfile;

establishing a relationship between a key identifier and the key stored in the keyfile;

storing the keyfile in one of,

an encrypted file in the database system, and

a location separate from the database system; and

moving an obfuscated copy of the keyfile to a volatile memory within a server associated with the database system.

40. (Previously presented) The computer-readable storage medium of claim 39, wherein the key identifier associated with the column is stored as metadata associated with a table containing the column within the database system.

41. (Previously presented) The computer-readable storage medium of claim 39, wherein the method further comprises establishing encryption parameters for the column, wherein encryption parameters include encryption mode, key length, and integrity type by:

entering encryption parameters for the column manually; and

recovering encryption parameters for the column from a profile table in the database system.

42. (Previously presented) The computer-readable storage medium of claim 35, wherein upon receiving a request from the security administrator specifying the column to be encrypted, if the column currently contains data, the method further comprises:

31

decrypting the column using an old key if the column was previously encrypted; and

encrypting the column using a new key.

43. (Currently amended) An apparatus that facilitates managing encryption within a database system, wherein encryption is performed automatically and transparently to a user of the database system, comprising:

a receiving mechanism that is configured to receive a request at the database system to store data in the database system;

wherein the request is directed to storing data in a portion of the database system that has been designated as encrypted;

a digest creating mechanism configured to create a digest of the data;

an encrypting mechanism that is configured to automatically encrypt data within the database system using an encryption function to produce an encrypted data; and

a storing mechanism that is configured to store the encrypted data in the database system;

wherein the digest is used to detect tampering with the encrypted data.

44. (Previously presented) The apparatus of claim 43,

wherein the portion of the database system that has been designated as encrypted includes a column of the database system;

wherein the encryption function uses a key stored in a keyfile managed by a security administrator; and

wherein the encrypted data is stored using a storage function of the database system.

B1

45. (Previously presented) The apparatus of claim 44, further comprising:

the receiving mechanism that is further configured to receive a request to retrieve data from the column of the database system;

an access mechanism that is configured to prevent a database administrator and the security administrator from decrypting the encrypted data; and

wherein the access mechanism is configured to allow an authorized user of the database system to decrypt the encrypted data.

46. (Previously presented) The apparatus of claim 44, further comprising a selection mechanism that is configured to select one of, data encryption standard (DES) and triple DES as a mode of encryption for the column.

47. (Previously presented) The apparatus of claim 44, wherein the security administrator, a database administrator, and a user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles.

48. (Previously presented) The apparatus of claim 44, further comprising:

a creating mechanism that is configured to create the keyfile;

an establishing mechanism that is configured to establish a plurality of keys to be stored in the keyfile;

wherein the establishing mechanism is further configured to establish a relationship between a key identifier and the key stored in the keyfile;

wherein the storing mechanism is further configured to store the keyfile in one of,

an encrypted file in the database system, and

a location separate from the database system; and

B1

a moving mechanism that is configured to move an obfuscated copy of the keyfile to a volatile memory within a server associated with the database system.

49. (Previously presented) The apparatus of claim 48, wherein the key identifier associated with the column is stored as metadata associated with a table containing the column within the database system.

50. (Previously presented) apparatus of claim 48, wherein the establishing mechanism is further configured to establish encryption parameters for the column, wherein encryption parameters include encryption mode, key length, and integrity type, and wherein the establishing mechanism includes:

an entering mechanism that is configured to enter encryption parameters for the column manually; and a recovering mechanism that is configured to recover encryption parameters for the column from a profile table in the database system.

51. (Previously presented) The apparatus of claim 44, further comprising:

a decrypting mechanism that is configured to decrypt the column using a previous key if the column was previously encrypted; and

B1

wherein the encrypting mechanism is further configured to encrypt the column using a new key.